AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Google accounts geezeepetes@gmail.com and wtedh78@gmail.com that is stored at Google LLC

Case No. 3:20mj133

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-1

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment C-1	

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig

Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 3/13/20

Judge's signature

City and state: Dayton, Ohio

Michael J. Newman, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-1

Information associated with the Google accounts **geezeepetes@gmail.com** and **wtedh78@gmail.com** that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B-1
Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

Email Accounts:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. The types of service utilized;
4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

Google Photo Accounts:

6. Subscriber registration information;
7. All photographs and videos currently or previously contained in the user's account or shared albums, to include deleted photographs and videos, and any associated file information;

Google Drive Accounts:

8. Subscriber registration information;
9. Any files created or previously contained in the user's account, to include deleted files, and any associated file information;
10. Any IP logs and other information associated with files from the account;

Web and App History:

11. Subscriber and registration information;
12. Any available Web and App History data;
13. Any IP logs associated with the Web and App History Data;

Google+:

14. Subscriber registration information;
15. Circle information to include name of Circle and members, contents of postings, comments, photographs, and time stamps;
16. Community information, to include name of Community and members, contents of Communities, and comments;
17. Hangout information, to include name of Hangouts and any preserved videos;
18. Any photographs and videos posted on the user's account and associated comments;
19. Any comments posted to other users' accounts.

Android Backup:

20. Any available backup data for any electronic devices.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. § 2251(a) and (e) (production of child pornography), 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography); involving WILLIAM THEODORE HALL from January 1, 2018 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, distribution, and production of child pornography.

2. Any visual depictions of minors, and any identifying information for these minors.

3. Any Internet or search history indicative of searching for child pornography or content involving children.

4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.

5. Any communications with minors, and any identifying information for these minors.

6. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.

7. Evidence of utilization of telephone accounts;

8. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.

9. Any information related to the use of aliases.

10. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-1

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession or Attempted Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt, Distribution, Attempted Receipt, and Attempted Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt, Distribution, Attempted Receipt, and Attempted Distribution of Child Pornography
18 U.S.C. § 2251(a) and (e)	Production of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by WILLIAM THEODORE HALL, commonly known as "TED" (hereinafter referred to as "HALL"). This Affidavit is submitted in support of Applications for search warrants for the following:

   a. Information associated with the Google accounts **geezeepetes@gmail.com** and **wtedh78@gmail.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-1); and

   b. Information associated with the Dropbox account associated with the email address **wtedh78@yahoo.com** that is stored at premises controlled by Dropbox Inc. (as more fully described in Attachment A-2).

3. The purpose of the Applications is to seize evidence of violations of the following:

   a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography;

   b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce; and

   c. 18 U.S.C. § 2251(a) and (e), which make it a crime to produce or attempt to produce child pornography.

4. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto and are incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 and A-2).

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), and 2251(a) and (e), are present within the information associated with the above noted accounts (as described in Attachments A-1 and A-2).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. § 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means,

including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

10. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

11. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

12. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

13. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

14. The following definitions apply to this Affidavit and Attachments B-1 and B-2 to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).

e. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

f. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

g. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

h. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

i. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Google Services

15. Google LLC is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.

16. Google Photos is a photograph and video sharing and storage service provided by Google LLC, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any telephone, tablet, or computer. It also allows users

to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.

17. Google+ is a social networking and identity service website owned and operated by Google LLC, located at www.plus.google.com. Common features include the following:

a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.

b. Circles: Google+ allows users to establish "circles", which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical "Friends" list function used by sites such as Facebook and MySpace.

c. Communities: Communities allow users with common interests to communicate with each other.

d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.

e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.

f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.

18. Google Web and App History is a feature of Google Search in which a user's search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user's Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.

19. Google Drive is a file storage and synchronization service provided by Google LLC, located at www.drive.google.com. This service provides cloud storage, file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.

20. Google Android Backup is a service provided by Google LLC to backup data connected to users' Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users' devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

Cloud Storage and Dropbox

21. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations.

22. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.'s servers. According to Dropbox Inc.'s privacy policy, at https://www.dropbox.com/privacy, Dropbox Inc. collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's IP address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service.

Collectors of Child Pornography

23. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to

seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Telegram Messenger

24. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.

25. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.

26. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram's special "secret" chats use end-to-end encryption, leaving no trace of the chat's on Telegram's servers. The secret chats provide users the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender's and receiver's devices when the timer expires.

27. Telegram users have the option to create a user name that is displayed to other users. User names are uniquely assigned on a first-come, first-serve basis. Users have the ability to conceal their user names from others so that they can utilize Telegram anonymously.

28. Based on my training and experience, I know that individuals involved in child pornography and child abuse offenses have utilized Telegram Messenger to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of offenders utilize Telegram's security features to avoid detection from law enforcement officers.

Other Social Media Applications

29. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

30. Grindr is a geospatial networking and online dating application geared towards gay, bi-sexual, and trans-sexual people. The application runs on iOS and Android mobile devices. It uses a mobile device's geolocation data to allow users to locate other users who are nearby.

31. WhatsApp is a freeware, cross-platform messaging and Voice over IP (VoIP) service owned by Facebook Inc. It allows users to send text messages and voice messages; make voice and video calls; and share images, documents, user locations, and other media. WhatsApp's client application runs on mobile devices but is also accessible from desktop computers that are connected to the Internet.

32. Based on my training and experience, I know that individuals involved in child pornography and child exploitation offenses have utilized various social media applications, including Grindr, WhatsApp, and Facebook, to trade child pornography files and to communicate with other offenders and victims.

FACTS SUPPORTING PROBABLE CAUSE

Information from Cooperating Witnesses

33. Beginning in or around December 2019, I have been involved in an investigation of child pornography offenses committed by an adult male who will be referred to for purposes of this Affidavit as "Adult Male A". On or around January 9, 2020, a federal search warrant was executed at Adult Male A's residence in Dayton, Ohio. Various electronic media were seized pursuant to the search warrant, including an Apple iPhone. A subsequent search of the iPhone revealed that Adult Male A had utilized the Telegram and WhatsApp Messenger applications to trade child pornography files with others and to discuss the sexual exploitation of children.

34. During the execution of the search warrant, Adult Male A agreed to be interviewed. I have also conducted several follow-up interviews of Adult Male A in or around January 2020. During these interviews, Adult Male A admitted that he utilized the Telegram Messenger application to trade child pornography files with others. Adult Male A identified that one of these individuals was an adult male who lived in or near Piqua, Ohio. Although Adult Male A could not recall this man's name, Adult Male A identified the man via photograph as HALL. Below is a summary of information that Adult Male A provided about HALL during the various interviews:

a. Adult Male A met HALL on the Grindr online dating application approximately one to two years ago, when Adult Male A was living in Piqua, Ohio. Prior to meeting HALL, Adult Male A had not been involved in child pornography offenses. HALL was the first person who sent Adult Male A child pornography files.

b. HALL first talked to Adult Male A about child pornography on the Grindr application. HALL then instructed Adult Male A to download the Telegram application, and they then began communicating on Telegram.

c. HALL sent Adult Male A images and videos depicting child pornography on the Telegram application. The children depicted in the child pornography files ranged from infant and toddler ages to teenagers. Adult Male A estimated that HALL sent Adult Male A these child pornography files on less than twenty-five occasions. HALL also invited Adult Male A into a group chat on Telegram that exchanged numerous child pornography files. New members could only be added into this group if they were invited into the group by an existing member.

i. Based on my training and experience, I know that some group chats on online messenger applications will only accept new members if existing members invite the new members into the group. In my experience, this

provides an added security feature to ensure that the new members are not affiliated with law enforcement.

d. HALL sometimes came over to Adult Male A's residence in Piqua, Ohio so that they could engage in sexually explicit conduct with each other. There were times when HALL watched videos depicting child pornography that he had on his cellular telephone while engaging in the sexual activities with Adult Male A. Adult Male A was able to see these videos and noted that they depicted HALL engaging in sexually explicit conduct with a male child. Conduct that Adult Male A observed in these videos included HALL touching and fondling the child's buttocks and/or genitals, the child touching HALL's buttocks and/or genitals, HALL providing oral sex to the child, and HALL receiving oral sex from the child.

i. Based on Adult Male A's descriptions of these videos, I believe that some or all of them depict child pornography. Given that HALL is depicted in the videos, it is reasonable to believe that he produced the videos.

e. Adult Male A first stated that he had seen at least two videos that depicted HALL engaging in sexually explicit conduct with the male child. Adult Male A later estimated that he had seen at least four of these videos. It appeared to Adult Male A that the boy depicted in the videos was approximately nine to ten years of age. Adult Male A could see HALL's face in the videos and felt confident that HALL was in fact depicted in the videos.

f. Adult Male A advised that HALL might have called the child depicted in the above described videos his nephew. HALL talked about baby-sitting the child on past occasions.

g. There was a time when Adult Male A met HALL at a Walmart store in or around Piqua, Ohio. HALL arrived at the store in a black truck. Adult Male A got into HALL's truck and saw that HALL had a small laptop with him. HALL showed Adult Male A child pornography files on this laptop. It appeared to Adult Male A that HALL had hundreds of child pornography files that were saved in a folder on the laptop. Adult Male A did not see any files on the laptop that depicted HALL engaging in sexually explicit conduct with children.

h. Adult Male A stopped communicating with HALL approximately one year ago, when Adult Male A moved out of his residence in Piqua, Ohio. Adult Male A has not received child pornography files from HALL since that time. Adult Male A periodically received messages from HALL over the past approximately one year via Grindr and Facebook, but Adult Male A did not respond to the messages. The

last message that Adult Male A received was in late January 2020 via Grindr. Adult Male identified that HALL's Grindr profile name at that time was "Nwor".

i. Adult Male A showed me HALL's profile picture as well as the message he received from HALL. I noted that the profile picture depicted the face of a white male wearing a hat and sunglasses. It appeared that HALL was the individual depicted in the photograph (although the hat and sunglasses prevented a more definitive identification).

i. HALL was previously on the Friends List of Adult Male A's Facebook account. Adult Male A could not recall HALL's Facebook account name.

j. Adult Male A provided a description of HALL that is consistent with HALL's physical appearance. Adult Male A was shown a photograph of HALL, and Adult Male A confirmed that the individual depicted in the photograph was HALL.

k. Adult Male A never communicated with HALL via telephone, and Adult Male A did not know HALL's telephone number.

l. Adult Male A had never been to HALL's residence. Based on HALL's comments, Adult Male A believed that HALL lived in Piqua, Ohio with a relative.

35. On or around November 29, 2019, an adult male who will be referred to for purposes of this Affidavit as "Adult Male B" submitted an online tip to the FBI's National Threat Operations Center (the FBI's telephone and online complaint system). Adult Male B reported that he recently met a man on the Grindr dating application, and that this man talked about molesting his nephew. I later conducted two interviews of Adult Male B in or around December 2019 and January 2020. Adult Male B reported that he knew the man he met on Grindr as "Teddy" (a common nickname for HALL's middle name, and similar to HALL's known alias, as detailed below). Adult Male B also positively identified HALL from a photographic lineup. The information that Adult Male B provided about HALL during the interviews is consistent with the information provided by Adult Male A. At this time, I am not aware of Adult Male A and Adult Male B being acquainted with each other.

36. In summary, Adult Male B provided the following information about HALL in his online complaint and during the two interviews:

a. Adult Male B met HALL in or around November 2019 on the Grindr dating application. HALL offered to provide drugs to Adult Male B, and they coordinated to meet with each other. HALL picked up Adult Male B in a dark

blue truck (similar to the vehicle Adult Male A saw HALL drive to the Walmart store, as detailed above). While they were in a parking lot, HALL and Adult Male A used a quantity of methamphetamine that HALL provided. HALL then drove Adult Male A to HALL's residence in Piqua, Ohio.

b. While at the residence, HALL took Adult Male B to a bedroom on the second floor. It was Adult Male B's understanding that this was HALL's bedroom. HALL and Adult Male B used an additional quantity of methamphetamine while in the bedroom, which was again provided by HALL.

c. HALL and Adult Male B engaged in sexual activities with each other in the bedroom. HALL also showed Adult Male B pornographic videos on HALL's cellular telephone. It appeared that HALL played or streamed these videos from a commercial website. HALL commented that he thought that some of the individuals depicted in the videos were juveniles, as he had seen them on the "dark web".

d. HALL made a number of sexually explicit comments about his nephew during the time that Adult Male B was at the residence. Comments that HALL made about his nephew included the following:

i. HALL indicated that he had been sexually active with his nephew for around five years. HALL also indicated that he had regular contact with his nephew.

ii. HALL made comments indicating he had provided oral sex to the nephew and that the nephew had provided oral sex to him.

iii. HALL said that his nephew had masturbated in front of him.

iv. HALL said that he "collected" things from his nephew.

v. HALL stated that he had several photographs depicting his nephew nude, but that he would only show Adult Male B one of these photographs.

e. HALL showed Adult Male B a photograph on HALL's cellular telephone. This photograph depicted a nude male child kneeling on his knees with his buttocks in the air. HALL said that the boy depicted in the photograph was his nephew. Adult Male B advised that based on the angle that the picture was taken, it was difficult to estimate the age of the boy depicted in the photograph. However, it appeared to Adult Male B that the individual depicted in the photograph could possibly be around sixteen to eighteen years of age.

f. HALL showed Adult Male B a pair of children's underwear that was on the dresser in the bedroom. HALL said that this underwear belonged to his nephew. The underwear appeared to be a size for a male child who was approximately six to eight years of age.

g. Adult Male B questioned HALL about HALL's possible sexual contact with children. Adult Male B asked if children were sexually different from adults, and HALL responded that they were. HALL commented that children also tasted differently. HALL made comments about wanting to "rape a young straight boy's ass" (or words to that effect) and to "eat a baby's ass" (or words to that effect).

h. As Adult Male B continued to ask HALL questions, HALL seemed to become paranoid. HALL then told Adult Male B to leave the house.

i. Approximately one month after meeting HALL, Adult Male B and HALL again communicated with each other via Grindr. Adult Male B met HALL again at HALL's residence. They used methamphetamine together in HALL's bedroom, but they did not engage in sexual activities with each other or talk about HALL's nephew.

j. Around mid-January 2020, Adult Male B sent HALL a message on Grindr asking how HALL was doing. HALL provided a curt response.

k. HALL and Adult Male B only communicated with each other via Grindr. Adult Male B did not know HALL's telephone number or Facebook account name.

l. Based on comments that HALL made, it was Adult Male B's understanding that HALL lived with his father. Adult Male B did not meet or see the father at the residence.

m. During an interview on or around January 30, 2020, Adult Male B accessed and showed me HALL's Grindr profile picture.

    i. I noted that HALL's profile name was "Nwor", and that it contained the same profile name and picture that Adult Male A had showed to me during one of his interviews (which was a few days prior).

n. Based on the description that Adult Male B provided of HALL's residence, Adult Male B was shown various photographs of residences that were in this geographic location. Adult Male B identified that photograph depicting the residence at 1435 Covington Avenue, Piqua, Ohio, 45356 (hereinafter referred to as the "SUBJECT PREMISES") was HALL's residence.

o. HALL made a comment on one occasion that he was employed as a bartender at the Masque night club in Dayton, Ohio

p. Adult Male B was shown a photographic lineup depicting six white males, one of whom was HALL. Adult Male B positively identified HALL from this lineup.

Records Related to HALL and SUBJECT PREMISES-1

37. Records from the Ohio Bureau of Motor Vehicles identified that HALL utilized SUBJECT PREMISES-1 when renewing his Ohio driver's license in 2016. His license was suspended in 2017 and has not been reinstated since that time. Records from the Miami County Auditor's Office identified that William M. HALL owns SUBJECT PREMISES-1. Based on his name and date of birth, it appears that William M. HALL is HALL's father or other relative.

38. Records from the Montgomery County (Ohio) Jail identified that HALL was arrested in or around July 2016 for a theft offense and in or around March 2017 for a drug offense. The arresting officers for both arrests noted that HALL's address was SUBJECT PREMISES-1 when booking him into the jail.

39. As part of the investigation, I obtained a report from the Piqua (Ohio) Police Department regarding suspicious activity at SUBJECT PREMISES-1 on or around August 12, 2019. According to the report, HALL called 911 from telephone number 937-381-7919 (hereinafter referred to as "CELL PHONE-1") and reported that someone had stolen the pump from the swimming pool that was on the property. The report identified that HALL used the name "TED" and that his cellular telephone number was 937-418-2403 (hereinafter referred to as "CELL PHONE-2").

a. It was noted that the telephone number that the officer listed for HALL in the report was different from the telephone number that HALL used to call 911. Based on my training and experience, I know the following:

i. When writing reports, law enforcement officers sometimes utilize the last known telephone numbers that are documented in the police department's records system if the officers were not able to obtain the person's telephone number during their contact with those individuals.

ii. Some individuals own and utilize multiple cellular telephones.

iii. In cases where individuals utilize their cellular telephones to conduct illegal activities, it is not uncommon for them to report false cellular telephone numbers to law enforcement officers.

Information and Records from Facebook

40. On or around February 19, 2020, I reviewed publicly available information on the Facebook website for possible accounts utilized by HALL. I located an account with a profile name of "TED HALL" and an account name of RitABee78. Although the current profile picture for the account depicted a generic picture, there were numerous former profile pictures and other photographs posted to the account that depicted HALL. Based on this and other information detailed in the Affidavit, I believe that HALL is the user of the RitABee78 Facebook account.

41. Consistent with the information provided by Adult Male B, the publicly available profile information for the RitABee78 Facebook account identified that HALL was formerly employed at the Masque night club. Review of historical information on the account's publicly available timeline revealed the following information:

a. On or around November 22, 2015, HALL posted a picture to his account that depicted him and a juvenile male child. This child appeared to be approximately four to six years of age and was wearing pajamas. HALL and the child appeared to be in the kitchen of a residence. HALL posted the following caption with the picture: "My nephew *[male name]*! This boy is growing so fast!!!".

b. On or around December 14, 2015, HALL changed the profile picture for his account. The new profile picture depicted HALL and the same juvenile male child from the picture posted on or around November 22, 2015. The child was wearing what appeared to be the same pajamas from the previous photograph, and HALL and the child appeared to be in the same kitchen.

42. As detailed above, approximately one to two years ago, Adult Male A observed child pornography videos on HALL's cellular telephone that depicted HALL engaging in sexually explicit conduct with a male child who appeared to be approximately nine to ten years old. Adult Male A believed that HALL referred to this child as HALL's nephew, and HALL talked about babysitting the child. Also as detailed above, HALL posted pictures of his purported nephew on his Facebook account in or around November and December 2015 (a few years prior to the child pornography videos Adult Male A observed on HALL's cellular telephone), and this boy appeared to be approximately four to six years old at that time. Based on this and other information detailed in the Affidavit, it is reasonable to believe that the child depicted on HALL's Facebook account might also be the same child depicted in the child pornography videos that Adult Male A observed on HALL's cellular telephone.

43. As part of the investigation, Facebook Inc. was served with two subpoenas requesting subscriber information for the RitABee78 Facebook account as well as logs of IP

addresses utilized to access the account. On or around February 25, 2020, Facebook Inc. was served with a search warrant authorized by the United States District Court for the Southern District of Ohio for information associated with the RitABee78 Facebook account. Facebook Inc. has produced and provided records in response to the subpoenas and search warrant. Review of these records provided the following information:

a. The account was created on or around January 24, 2009, in the name of "TED HALL". The email address of **wtedh78@yahoo.com** was the registered email address for the account.

b. The date of birth listed for the account user matches HALL's date of birth. The user listed that the current city where he resides is Piqua, Ohio (consistent with SUBJECT PREMISES-1).

c. The following cellular telephone numbers were associated with the RitABee78 Facebook account: CELL PHONE-1, CELL PHONE-2, 937-214-0594 (hereinafter referred to as "CELL PHONE-3"), and 937-418-8611 (hereinafter referred to as "CELL PHONE-4"). Facebook Inc.'s records identified that these numbers were "verified" in that the account user had responded to text messages that Facebook Inc. had sent to the user.

d. Facebook Inc. provided a log of IP addresses that had been utilized to log into and out of the RitABee78 Facebook account during the approximate time period of July 13, 2019 through March 2, 2020. This log provided the following information:

   i. From approximately October 17, 2019 through March 2, 2020, the only IP addresses utilized to access the RitABee78 Facebook account were IP addresses serviced by Sprint Corporation and Charter Communications. The use of IP addresses serviced by Sprint Corporation is consistent with someone using the data plan from his/her cellular telephone to access his/her Facebook account. The use of IP addresses serviced by Charter Communications is consistent with someone using wireless Internet service at a residential or business location to access his/her Facebook account.

   ii. From approximately July 13, 2019 through September 22, 2019, the only IP addresses utilized to access the RitABee78 Facebook account were IP addresses serviced by AT&T Mobility and Charter Communications. The use of IP addresses serviced by AT&T Mobility is again consistent with someone using the data plan from his/her cellular telephone to access his/her Facebook account.

e. When exchanging messages with other users via Facebook's Messenger application, HALL made various comments about one or more of his nephews on approximately fifty-three occasions. Consistent with the information provided by Adult Male A, HALL discussed watching his nephews on a number of occasions. HALL also made comments indicating that he previously lived with his father, sister, and nephews. Below are examples of some of these comments:

i. On or around September 17, 2018, HALL told the following to another user: "I live with my dad and my sister w 2 nephews.. 5 yo 7 yo".

ii. On or around April 20, 2019, HALL told the following to another user: "Watching my nephew".

iii. On or around July 24, 2019, HALL told the following to another user: "Unfortunately you can't come to my place right now because my nephews are there".

iv. On or around October 26, 2019, HALL told the following to another user: "Just picked up my nephews". HALL then sent a photograph to the other user depicting two male children sitting in what appeared to be the back seat of a vehicle.

v. Again on or around October 26, 2019, HALL told the following to another user: "Considering I'm with my 7 and 9 yo nephews probably not".

vi. On or around December 26, 2019, HALL told the following to another user: "I'm headed to see my nephews".

f. In messages exchanged with other users via Facebook's Messenger application, HALL made various comments indicating that he lived with his father. Beginning on or around December 21, 2019, HALL told at least approximately seven other users that his father had recently moved in with HALL's sister. In some of the messages, HALL indicated that he was now living alone. Below are a few examples of these comments:

i. On or around December 21, 2019, HALL told the following to another user: "Don't need help anymore guess my dads moving in with my sister so I'm going to fix up the downstairs and close off the second floor".

ii. On or around December 25, 2020, HALL told the following to another user: "My dad went to live with my sister this big ass house fallen in on me".

iii. On or around January 18, 2020, HALL told the following to another user: "Not bad. Just got home. My dad moved in with my sister so I went to see them. Now I'm in this bigass house alone. Kinda weird".

g. During the approximate time period of November 2018 through July 2019, HALL sent messages to three other users indicating that his telephone number was CELL PHONE-3. On or around September 22, 2019, HALL sent a message to another user in which he indicated that he was using his father's telephone. On or around January 22, 2020, when another user was attempting to call HALL via Facebook Messenger, HALL responded by stating "937-606-0594 my private line".

h. On or around June 3, 2019, HALL sent a picture of Adult Male A to another user, along with the following message: "My year long crush".

i. During the approximate time period of July 2018 through February 2020, HALL exchanged various messages with another user utilizing the display name of "William Clemens" (hereinafter referred to as "CLEMENS"). Based on these messages, it appeared that HALL and CLEMENS were involved in a sexual relationship and that CLEMENS helped pay for some of HALL's expenses.

Subpoenas to Telephone Providers

44. Sprint Corporation was identified as the service provider for the CELL PHONE-1. On or around January 29, 2020, Sprint Corporation was served with a subpoena requesting subscriber information for the CELL PHONE-1. Records received in response to the subpoena identified that the CELL PHONE-1 was subscribed to CLEMENS (the name of the individual who HALL communicated with on Facebook, as detailed above) at 1433 Covington Avenue, Apartment 8D, Piqua, Ohio (which is located in a building directly behind SUBJECT PREMISES-1, and hereinafter referred to as "SUBJECT PREMISES-2"). However, the billing address for the account was SUBJECT PREMISES-1. The account was activated on or around September 28, 2019.

45. Verizon was identified as the service provider for CELL PHONE-2. On or around January 29, 2020, Verizon was served with a subpoena requesting subscriber information for CELL PHONE-2. Records received in response to the subpoena identified that the number belonged to a TracFone[1], and that no subscriber information was maintained by Verizon for the account.

1 TracFone Wireless Inc. is an American prepaid, no-contract mobile phone provider. TracFone Wireless operates as a mobile virtual network operator, holding agreements with other wireless network operators (including Verizon, AT&T Mobility, T-Mobile, Sprint Corporation, and U.S. Cellular) to provide service to its customers.

46. AT&T was identified as the service provider for CELL PHONE-3. On or around February 21, 2020, a subpoena was served to AT&T requesting subscriber information for CELL PHONE-3. Records received in response to the subpoena identified that the financial and billing party for the account was CLEMENS, and the user name for the account was "God God". The address listed for both CLEMENS and "God God" was SUBJECT PREMISES-1. The email address listed for both CLEMENS and "God God" was **wtedh78@yahoo.com** (the same email address associated with HALL's Facebook account). The account was cancelled on or around October 27, 2019 (consistent with the IP logs provided by Facebook Inc.).

47. Verizon was identified as the service provider for CELL PHONE-4. On or around February 21, 2020, a subpoena was served to Verizon for CELL PHONE-4. Records received in response to the subpoena identified that the number was subscribed to Ronald Harvey at an address in Troy, Ohio.

Records from Charter Communications

48. As part of the investigation, four subpoenas were served to Charter Communications for a sample of nine of the IP addresses that were utilized to access the RitABee78 Facebook account (as obtained from the records provided by Facebook Inc. in response to the search warrant and subpoenas detailed above). Records received from Charter Communications in response to the subpoenas provided the following information:

a. Two of the IP addresses, which were utilized to access the RitABee78 Facebook account on or around September 23, 2019 and September 29, 2019, were subscribed to "WILLIAM HALL" at SUBJECT PREMISES-1. CELL PHONE-3 and the email address of **wtedh78@yahoo.com** (the same email address associated with HALL's Facebook account and the subscriber information for CELL PHONE-3) were listed as contact information for the subscriber. Records from Charter Communications Inc. identified that this account is presently closed.

b. Seven of the IP addresses, which were utilized to access the RitABee78 Facebook account during the approximate time period of November 27, 2019 through March 2, 2020, were subscribed to CLEMENS at SUBJECT PREMISES-2. Records from Charter Communications identified that this account was active as of on or around March 6, 2020.

49. As noted above, SUBJECT PREMISES-2 is located in a building directly behind SUBJECT PREMISES-1. On or around March 3, 2020, I sat in a public business parking lot that is located next to SUBJECT PREMISES-1. I utilized a cellular telephone to scan for wireless Internet service that was accessible to me at my location. Among other accounts, I located a wireless Internet account with an account name of "ClemensWiFi". Based on the account name, it is reasonable to believe that this Internet account belongs

to CLEMENS at SUBJECT PREMISES-2. The distance between my location and SUBJECT PREMISES-2 was greater than the distance between SUBJECT PREMISES-1 and SUBJECT PREMISES-2. It is therefore reasonable to believe that an individual residing at SUBJECT PREMISES-1 could access the wireless Internet service at SUBJECT PREMISES-2.

50. Based on my training and experience, I know that individuals living in close proximity to each other sometimes share wireless Internet service as a cost savings mechanism. Based on the information detailed above, it is reasonable to believe that HALL is currently using the wireless Internet service at SUBJECT PREMISES-2.

Surveillance Activity

51. On or around March 3, 2020, I conducted surveillance of SUBJECT PREMISES-1 and SUBJECT PREMISES-2. During the early evening hours, I observed the following activity:

a. A white male exited the door on the east side of SUBJECT PREMISES-1 and walked directly into the entry door for SUBJECT PREMISES-2 without knocking. The approximate height, weight, and hair color for this individual appeared to be consistent with HALL. However, given the minimal daylight, I was unable to positively identify this individual as HALL.

b. After the white male entered SUBJECT PREMISES-2, I periodically observed small flashes of light through the window next to the entry door. These flashes of light were consistent with the light that could be coming from the screen of a cellular telephone.

c. Approximately twenty minutes after the white male entered SUBJECT PREMISES-2, I observed an individual walking around behind SUBJECT PREMISES-1. This individual then appeared to walk around to the front of SUBJECT PREMISES-1, at which time he/she sat on the porch.

d. Approximately four minutes later, a white male exited SUBJECT PREMISES-2. The height, weight, and hair color of this individual were again consistent with HALL, but I was unable to make a positive identification due to the lack of daylight. The white male returned to SUBJECT PREMISES-1, and both he and the other individual sitting on the porch entered the door on the east side of the residence.

52. On or around March 9, 2020, I again conducted surveillance of SUBJECT PREMISES-1 and SUBJECT PREMISES-2. During the early evening hours, I observed the following activity:

a. During the early evening hours, a blue Chevrolet Silverado truck registered to CLEMENS pulled into the parking lot for SUBJECT PREMISES-2 and parked near SUBJECT PREMISES-2. An individual who appeared to be CLEMENS exited SUBJECT PREMISES-2 and approached the vehicle. An individual who appeared to be HALL then got out of the vehicle and walked into the door on the east side of SUBJECT PREMISES-1.

i. The individual who got out of the Chevrolet Silverado truck appeared to be HALL. Because the individual was wearing a hat, which obscured some of his facial features, I could not identify him as HALL with complete certainty.

ii. As detailed above, Adult Male B identified that HALL picked him up in or around November 2019 in a dark blue truck (which is consistent with the Chevrolet Silverado truck).

b. A few minutes later, the individual who appeared to be HALL exited the door on the east side of SUBJECT PREMISES-1 and returned to the Chevrolet Silverado truck, where he appeared to interact with CLEMENS. The individual who appeared to be HALL then returned to SUBJECT PREMISES-1 and entered the door on the east side of the residence. The individual who appeared to be CLEMENS remained standing by the vehicle for a short time and then returned to SUBJECT PREMISES-2.

Information from Telegram

53. On or around February 21, 2020, an FBI investigator searched publicly available information on the Telegram application for accounts associated with the CELL PHONE-1, CELL PHONE-2, CELL PHONE-3, and CELL PHONE-4. The investigator found that there were Telegram accounts associated with the CELL PHONE-1 and CELL PHONE-3. The Telegram account associated with the CELL PHONE-1 had a display name of "TED HALL", and it was presently offline. The Telegram account associated with CELL PHONE-3 had a display name of "MarsHALL78 HaWl".

a. As detailed above, Adult Male A identified that he previously communicated with and received child pornography files from HALL via Telegram.

Execution of Search Warrant at SUBJECT PREMISES-1

54. On or around March 11, 2020, agents and task force officers of the FBI searched SUBJECT PREMISES-1 pursuant to a search warrant authorized by the United States District Court for the Southern District of Ohio. HALL was the only individual present

when agents and officers arrived to execute the warrant. Various computer media were seized from the residence pursuant to the warrant, including an LG cellular telephone, two laptops, and a cellular telephone that appeared to be burned.

55. Pursuant to the search warrant, a preliminary examination has been conducted of the LG cellular telephone. Below is a summary of information obtained during the preliminary examination:

a. The telephone number for the device was 937-214-0155 (hereinafter referred to as "CELL PHONE-5").

b. The dates associated with the call logs, text messages, images, and videos that were saved on the device indicated that it had only been used since on or around March 1. 2020.

c. No child pornography files were recovered from the device.

d. Two email accounts were established on the device: **geezeepetes@gmail.com** and **wtedh78@gmail.com**. Email messages sent to and from these email accounts were saved on the device. These emails included the following:

i. A number of emails were sent to the **wtedh78@gmail.com** account that were from email addresses associated with Google LLC. These emails provided the user with various notifications about the use of the **wtedh78@gmail.com** account. These notifications indicated that various Google products had been set up on a new Samsung Galaxy S10 cellular telephone in or around October and November 2019, including Gmail, Chrome, Google Photos, and YouTube.

1. Based on this and other information detailed in the Affidavit, it is reasonable to believe that the **wtedh78@gmail.com** email account contains information about the prior use of a Samsung Galaxy S10 cellular telephone, to potentially include photographs that were taken on the device and backed up to the Google Photos account.

ii. A number of emails were sent to the **geezeepetes@gmail.com** account that were from email addresses associated with various social media and electronic service providers, including Facebook and Tumblr. These emails indicated that the **geezeepetes@gmail.com** email account had been utilized to register accounts on these websites.

e. A number of images and videos depicting HALL was saved on the device.

Interviews of Other Witnesses

56. On or around March 11, 2020, CLEMENS was contacted and interviewed at SUBJECT PREMISES-2. A second, brief telephonic interview was conducted of CLEMENS on or around March 12, 2020. In summary, CLEMENS provided the following information during the two interviews:

a. CLEMENS had known HALL for approximately five years. They were presently involved in a sexual relationship.

b. HALL previously purchased three cellular telephones. He kept one of the cellular telephones for himself and gave the other two telephones to his father and to CLEMENS. The cellular telephone that HALL gave to CLEMENS was a white LG cellular telephone (consistent with the LG cellular telephone seized from HALL's residence pursuant to the search warrant). Approximately two weeks ago, HALL broke the cellular telephone that he was utilizing. CLEMENS gave HALL the white LG cellular telephone, and HALL has utilized it since that time.

i. The information CLEMENS provided about HALL's limited use of the LG cellular telephone is consistent with the minimal data recovered from the LC cellular telephone that was seized from SUBJECT PREMISES-1.

c. HALL's current cellular telephone number was CELL PHONE-5 (the number recovered from the LG cellular telephone seized from SUBJECT PREMISES-1). HALL's previous cellular telephone number was CELL PHONE-3 (one of the telephone numbers associated with the RitABee78 Facebook account).

d. HALL had a laptop that recently was broken or stopped working. Approximately two weeks ago, HALL began borrowing CLEMENS' Acer All-in-One computer. HALL sometimes took this computer back to SUBJECT PREMISES-1 and used it for periods of a few hours at a time. HALL told CLEMENS that he used the Acer All-in-One computer to work on his rap music.

57. On or around March 11, 2020, CLEMENS voluntarily turned over the Acer All-in-One computer to officers and provided his consent for officers to forensically examine it. Prior to turning over the device, CLEMENS showed officers the home screen or desktop of the device. Officers noted that a picture of HALL was contained on the home screen. The device was powered off at that time and was seized by officers.

58. The Acer All-in-One computer is currently secured at the FBI's office in Dayton, Ohio. It has not been accessed since it has been in law enforcement's possession.

59. The investigation has determined that HALL has a sister who will be referred to for purposes of this Affidavit as "Adult Female A". Adult Female A was contacted and interviewed on or around March 11, 2020. In summary, Adult Female A provided the following information:

a. Adult Female A had five sons who ranged in ages from six years old to twenty-one years old. Adult Female A also had a daughter who was presently an adult.

b. Adult Female A and her two youngest sons moved into SUBJECT PREMISES-1 approximately four years ago. They lived at the residence with HALL and their father on and off for a period of approximately three years. Adult Female A's three oldest sons periodically came over to the house during that time period to visit.

c. Adult Female A's sons (i.e., HALL's nephews) continued to spend time with HALL even after they moved out of SUBJECT PREMISES-1. HALL seemed to love spending time with his nephews.

d. During the previous year, Adult Female A found that one of her sons (who will be referred to for purposes of this Affidavit as "Minor A") was masturbating with a toy. When Adult Female A questioned what Minor A was doing, he said that HALL had taught him how to do this. Adult Female A became very upset, and Minor A then provided a different reason for why he was masturbating.

i. Based on my training and experience, I know that it is not uncommon for child victims of sexual abuse to recant their disclosures, particularly when the disclosures cause distress for their family members.

e. Adult Female A noted that approximately two years ago, while they were living at SUBJECT PREMISES-1, Minor A's behavior suddenly and drastically changed.

i. Based on my training and experience, I know that sudden and drastic changes in behavior of children could be one indicator of sexual abuse.

f. Approximately four to five years ago, Adult Female A's daughter stopped talking to HALL. Her daughter said that she was upset about videos that HALL posted to his Facebook account. Her daughter only said that the videos showed HALL in the shower and her brothers in the background, but neither she nor HALL would provide any details about these videos.

g. HALL previously created some videos that depicted two of Adult Female A's sons and posted them on the TikTok application (an online video-sharing social

networking service). Adult Female A did not observe any inappropriate content on these videos.

Records from Dropbox Inc.

60. On or around February 24, 2020, Dropbox Inc. was served with a subpoena requesting subscriber information and IP logs for any Dropbox accounts associated with the email address **wtedh78@yahoo.com**. Records received in response to the subpoena identified that a Dropbox account associated with the email address **wtedh78@yahoo.com** was created on or around April 25, 2014 in the name of "W-Ted Hall". The last authenticated login to the account was on or around December 3, 2019. The log of IP addresses utilized to access the Dropbox account included approximately four IP addresses serviced by Sprint Corporation.

a. The use of IP addresses serviced by Sprint Corporation is consistent with someone using the data plan from his/her cellular telephone to access his/her Dropbox account.

Conclusion Regarding Use of Accounts

61. Based on all of the information detailed in the Affidavit, I submit that there is probable cause to believe the following:

a. HALL has engaged in sexually explicit conduct with one of his nephews and has produced child pornography depicting this conduct. Evidence of this production of child pornography is contained on one or more of HALL's cellular telephones.

b. HALL has utilized the Telegram application to distribute and receive child pornography files. He has utilized at least two cellular telephone numbers to access his Telegram accounts.

c. HALL has possessed child pornography files on at least two devices – that being one of his cellular telephones and a laptop computer.

d. HALL is the user of the "Nwor" Grindr account. HALL has utilized the Grindr dating website to meet at least some of the individuals to whom he has distributed child pornography files and with whom he has discussed the sexual exploitation of children.

e. HALL is the user of the RitABee78 Facebook account, and he has utilized this Facebook account to post pictures of and talk about his nephews. He has also utilized this Facebook account to contact at least one of the individuals to whom

he distributed child pornography files (that being Adult Male A). Based on all of the information detailed in the Affidavit, it is reasonable the RitABee78 Facebook account contains information about the victims and co-conspirators of HALL's child pornography activities.

f. HALL is the user of the **wtedh78@yahoo.com** email account, and he has utilized this email account to register his Facebook account, Dropbox account, and potentially other social media accounts.

g. HALL is the user of the **wtedh78@gmail.com** and **geezeepetes@gmail.com** Google accounts. These Google accounts may contain evidence regarding the use and contents of his previous cellular telephones as well as other social media accounts that he has utilized.

h. HALL is the user of the Dropbox account associated with the email address **wtedh78@yahoo.com**. Based on all of the information detailed in the Affidavit (including information detailed below), it is reasonable to believe that this Dropbox account may contain evidence of HALL's child pornography and child exploitation activities.

i. HALL has utilized CLEMENS' Acer All-in-One computer, and this device might contain evidence of HALL's child exploitation activities.

Evidence Available in Email and Social Media Accounts

62. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

63. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

64. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat

programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

65. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.

66. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

67. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography and child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

68. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

69. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

70. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.

71. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

72. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

Evidence Sought in Searches of Dropbox Accounts

73. Dropbox and other cloud storage services provide a means that individuals can use to store files. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

74. Based on information received from Dropbox Inc., I know that Dropbox Inc. maintains basic subscriber information for its users, including user names, email addresses, and the dates that they established their accounts. Dropbox Inc. also maintains payment information, including credit card numbers, when payments are made on the accounts. Such information can provide material evidence regarding individuals involved in child pornography offenses, because this information can help identify the subjects and determine what aliases and email accounts they utilize. In addition, the dates that the accounts were established can help in identifying the length of time that the criminal activities transpired.

75. In addition to maintaining the files themselves, Dropbox Inc. also maintains files documenting various activities associated with its accounts. One such file is entitled "uploadlog.html". This file maintains information about the account name, computer name, and dates that files were uploaded, deleted, and modified. Such information provides material evidence to child pornography investigations, as the information helps identify the computer devices utilized by the subjects and when and how the files were received.

76. Another file maintained by Dropbox Inc. for its accounts is entitled "auth.txt". This file maintains logs of IP addresses and devices utilized to access the account. Such information is important to child pornography investigations because it helps to establish the subjects' identities, what computer devices are utilized, where the subjects' computers are located, and when the criminal activities transpired.

77. A file entitled "links.txt" is another example of a file maintained by Dropbox Inc. for its accounts. This file maintains information about files being shared by the user. In cases involving the trading of child pornography, information about the shared files can be useful in helping to identify the subjects' trading activities.

78. Dropbox Inc. maintains various information about the settings for its users' accounts. Such settings include information about computers and other devices linked to the accounts. Information about what computers and devices are utilized by the subjects is again materially important to child pornography investigations.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

79. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Dropbox Inc. and Google LLC to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

CONCLUSION

80. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located in the accounts described in Attachments A-1 and A-2, including the following offenses: 18 U.S.C. §§

2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), and 2251(a) and (e).

81. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.

82. Because the warrants for the accounts described in Attachments A-1 and A-2 will be served on Dropbox Inc. and Google LLC, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 13th of March 2020

MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE COURT JUDGE